IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:

Philip Hawkes et al..

Serial No.: 09/933,972

Filed: August 20, 2001

For: METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM

Examiner: Michael Simitoski

Group Art Unit: 2134

Attorney Docket No.: 010497

ELECTRONIC FILING

Transmitted electronically to the Patent and Trademark Office.

Depositor's Name: *Tram Q. Le*

Date: January 22, 2008

Signature: /Tram Q. Le/

REPLY BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attention: Board of Patent Appeals and Interferences

Sirs:

This Reply Brief is submitted pursuant to 37 C.F.R. § 41.41 in response to the Examiner's Answer mailed November 19, 2007. This Reply Brief is submitted within two months of the mailing date of the Examiner's Answer pursuant to 37 C.F.R. § 41.41(a)(1).

APPELLANT'S REPLY TO EXAMINER'S RESPONSE TO ARGUMENT

As set forth in detail in Appellant's Appeal Brief, Appellant maintains that the Examiner has, at least, failed to establish anticipation under 35 U.S.C. § 102 based on the cited reference, namely U.S. Patent No. 6,690,795 to Richards et al. ("Richards") because the cited reference does not describe the identical invention in as complete detail as contained in the claims as is required for a proper anticipation rejection. Appellant respectfully reminds the Examiner that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Brothers v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Furthermore, the identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

The anticipation rejections under 35 U.S.C. §102 are further argued herein as Appellant's independent claims 1, 11, 15, and 22-24 were rejected under 35 U.S.C. §102 and not under 35 U.S.C. §103. Accordingly, the obviousness rejections were argued in Appellant's Appeal Brief and are not further argued herein.

The teachings of the cited references are as summarized on Appellant's Appeal Brief.

Rejection of Independent Claims 1, 11, 15, and 22-24 under 35 U.S.C. § 102

Claims 1-5, 10-11, 13-16 and 18-24 stand rejected under 35 U.S.C. § 102(b) as being unpatentable over Richards. Appellant respectfully traverses this rejection, as hereinafter set forth. Appellant asserts that Richards does not and cannot anticipate under 35 U.S.C. § 102 the

presently claimed invention of independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24 because Richards does not describe, either expressly or inherently, the identical inventions in as complete detail as are contained in the claims.

(1) The Examiner's Answer states:

> Richards' Fig. 26 discloses the general concept of Richards, where CCK_1, encrypted by UEV is provide to the set top box, and the *set top box uses UEV (something it already has)* to *decrypt [CCK_1]UEV to recover CCK_1* (#133). CCK_1 is then used to decrypt a copy of itself (#138), which is not pertinent to the present rejection. In step 144, the previously-recovered CCK_1 is used to decrypt the package [PK]CCK_1 to recover PK. In step 152, the previously-recovered *PK is used to decrypt the package [SK]PK to recover SK*. In step 165, the previously-recovered *SK is used to decrypt the package [CONTENT]SK to recover CONTENT*. (Examiner's Answer, p. 7; emphasis added).

Therefore, according to the disclosure of Richards in Fig. 26, as interpreted by the Examiner as applied, for example, to Appellant's independent claim 1, Appellant summarizes the distinctions in the following table.

Appellant's Claim 1	**Richards according to Examiner's Answer**
"a registration key specific to a participant"	"set top box uses UEV (something it already has)" Note-Examiner equates Richards' UEV to Appellant's "registration key"
"encrypting the first key with the registration key"	"decrypt [CCK_1]UEV to recover CCK_1" Note-Examiner equates Richards' CCK_1 to Appellant's "first key"
	"CCK_1 is used to decrypt the package [PK]CCK_1 to recover PK" Note-Richards' "first key" is used to decrypt some "interim" key, PK.
"determining a second key for decrypting content … encrypting the second key with the first key"	"PK is used to decrypt the package [SK]PK to recover SK … SK is used to decrypt the package [CONTENT]SK to recover CONTENT" Note-Examiner equates Richards' SK key for decrypting content to Appellant's "second key for decrypting content." Note-Richards' SK key for decrypting content was encrypted using the "interim" key, PK, and **not** the "first key", CCK_1 as claimed by Appellant.

As noted, Richards' "alleged second key", SK, (for decrypting content) is encrypted by an "interim" key, PK, which is further encrypted by Richards' "alleged first key", CCK_1, which is yet further encrypted by Richards' "alleged registration key", UEV. Clearly, Richards does **not** disclose Appellant's claimed invention including "encrypting the second key with the first key" and "encrypting the first key with the registration key". Accordingly, such claims are allowable over the cited prior art and Appellant respectfully requests the Board reverse the rejections of independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and

claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24.

(2) The Examiner's Answer then states:

> Appellant argues that PK and SK are not both encrypted by CCK_1. However, CCK_1 is required to recover PK, which is required to recover SK (col., lines 26-28). Without CCK_1, the value of SK would remain scrambled. CCK_1 directly encrypting PK and PK encrypting SK represents CCK_1 encrypting PK and SK, but the mathematical process takes multiple steps. (Examiner's Answer, p. 7; emphasis added).

Appellant respectfully disagrees. Appellant's claim, for example claim 1, clearly recites, "determining a second key for decrypting content … encrypting the second key with the first key" and "encrypting the first key with the registration key". In contrast and according to the Examiner's own interpretation above, Richards unequivocally discloses "PK is used to decrypt … SK [which] is used to decrypt the … CONTENT" and Richards "uses UEV (something it already has) to decrypt [CCK_1]UEV to recover CCK_1". (Examiner's Answer, p. 7). Clearly, Richards does **not** disclose using the CCK_1 to decrypt the content decryption key, SK.

The Examiner's argument that "the mathematical process takes multiple steps" is unfounded. Specifically, Appellant's claim, for example claim 1, clearly recites, that the second key, namely the key for decrypting content, is unequivocally "encrypt[ed] []with the first key" or in other words, the first key encrypts the second (content) key. According to the Examiner's "multiple step" argument, Richards' first key (CCK_1) **never** encrypts the second content key (SK) but instead, Richards' first key (CCK_1) ***encrypts some encrypted combination*** of the second key (SK) encrypted by an interim key (PK). Accordingly, Richards clearly does **not**

disclose that the first key (CCK_1) ever encrypts the second content key (SK). Accordingly, such claims are allowable over the cited prior art and Appellant respectfully requests the Board reverse the rejections of independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24.

(3) The Examiner's Answer then states:

> Appellant's brief (p. 13, ¶2-p. 14 ¶1) argues that the claimed "second key" cannot be equated to Richards' "SK and PK" because SK and PK are two values. However, further in the claim it is seen that Appellant is in fact claiming that the second key is represented by two, ***separately-updatable, parts***. Further, Fig. 20 & accompanying disclos[ure] col. 12, lines 18-20 shows that at some points, both SK and PK are ***updates***. Therefore, this ***argument is contradictory***. (Examiner's Answer, p. 8; emphasis added).

Appellant respectfully submits that the Examiner is confusing separate processes, namely, (1) encrypting/decrypting content and (2) updating keys. While Appellant may claim "separately-updateable parts", Appellant is not claiming separable encrypting and decrypting parts. Accordingly, Appellant's arguments are, in fact, **not** "contradictory" as alleged.

(4) The Examiner's Answer then states:

> Further, Appellant argues that "SK and PK" does not decrypt content, as claimed. However, similarly to the previous response, it is the Examiner's submission that because the ***CONTENT is directly decrypting using SK***, which must be ***itself decrypted using PK, then the key "SK and PK" is encrypting the content.*** Without PK, the content could not be decrypted (see Fig. 26, #152 and #159). (Examiner's Answer, p. 8; emphasis added).

Appellant respectfully asserts that those of ordinary skill in the art of cryptography know

that "keys" generally fall into one of two categories, namely, (1) key encrypting keys, meaning keys that are used to encrypt/decrypt "keys", and (2) data or content keys that are used to encrypt/decrypt data or content. Accordingly, it is completely unreasonable to imply that keys used to encrypt/decrypt other keys also "encrypt[] the content." (Examiner's Answer, p. 8). Furthermore, advancing the Examiner's argument to the next logical step would mean that Richards' UEV "provided to the set top box" "encrypt[s] the content [since] [w]ithout [UEV], the content could not be decrypted." (Examiner's Answer, p. 8). Such imagined extensions of logic are neither disclosed in Richards, nor known by those of ordinary skill in the art.

Appellant respectfully returns the argument to the legal standard for anticipation under 35 U.S.C. §102, namely, that the identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Appellant respectfully maintains that Richards clearly does **not** disclose that a first key (e.g., CCK_1) **ever** encrypts the second content key (e.g., SK). Accordingly, such claims are allowable over the cited prior art and Appellant respectfully requests the Board reverse the rejections of independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24.

Therefore, Appellant's independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24, cannot be anticipated under 35 U.S.C. § 102 by Richards. Accordingly, such claims are allowable over the cited prior

art and Appellant respectfully requests the Board reverse the rejections of independent claim 1 and claims 2-5 depending therefrom, independent claim 11 and claims 13 and 14 depending therefrom, independent claim 15 and claims 16 and 18-21 depending therefrom and independent claims 22-24.

Furthermore, the nonobviousness of independent claim 1 precludes a rejection of claim 6 which depends therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Appellant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claim 6 which depends from independent claim 1.

Furthermore, the nonobviousness of independent claim 1 precludes a rejection of claims 7-9 which depend therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Appellant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejection to claims 7-9 which depend from independent claim 1.

Furthermore, the nonobviousness of independent claims 11 and 15 preclude a rejection of claims 12 and 17 which respectively depend therefrom because a dependent claim is obvious only if the independent claim from which it depends is obvious. *See* In re Fine, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988), *see also* MPEP § 2143.03. Therefore, the Appellant requests that the Examiner withdraw the 35 U.S.C. § 103(a) obviousness rejections to claims 12 and 17 which respectively depend from independent claims 11 and 15.

CONCLUSION

Pursuant to 37 C.F.R. § 41.43(a)(1), Appellant respectfully requests acknowledgement of receipt and entry of this Reply Brief.

Appellant respectfully submits that claims 1-24 are allowable. Appellant respectfully requests the reversal of the rejections of currently pending claims 1-24 for the reasons set forth above.

Respectfully submitted,

Dated: January 22, 2008

By: /Won Tae C. Kim/

Won Tae C. Kim, Reg. No. 40,457
(858) 651-6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502